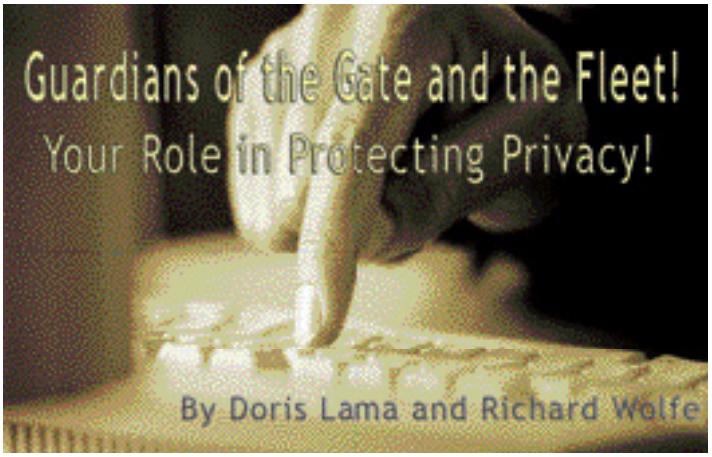

Consider this scenario: a major university in the Eastern United States finds that its Naval Reserve Officer Training Corps information site is hacked. Important private information pertaining to enrollees is stolen. The information is posted to a popular Web site and exposed to a huge audience. The hacker also posts how it was done and invites others to duplicate the theft at their institutions. Sound like a science fiction tale? No, it really happened not too long ago!

Many federal agencies have had the misfortune of reporting the loss of personally identifiable information (PII)— information that pertains to individuals, such as their name, Social Security Number (SSN), salary, and more. Recently, one breach involved the theft of 1.3 million medical records!

Here are a few more breaches that have recently occurred:

- A Navy recruiting station reported that 31,000 individuals were impacted when two legacy laptops were stolen from its office.
- A Naval Hospital Corps School reported that 60 to 70 students were impacted when a portable data storage device was stolen along with other personal effects from an office desk drawer during normal working hours.
- A command career counselor reported that 117 Selected Reservists were impacted when his car, which contained both a laptop and thumb drive containing personnel information, was stolen.

Your Help is Needed!

The Department of the Navy (DON) needs your help in protecting private information — your own and your teammates'! Personal information breaches cost money, which is not budgeted; time to perform a myriad of administrative functions; frustration — because you will have to explain what happened; and embarrassment — to you and your organization because it happened on your watch.

The purpose of this article is to ask you to factor in privacy safeguards as you do your job. Think about your role in this effort. When you came into the government as a civilian or contractor employee, or joined the military, you knew that as a condition of your employment you would need to provide personal information about yourself.

If you were appointed to a high level position, you were required to share financial information; if you required a security clearance, you had to provide lots of personal information — much more than just the basic name, SSN and date of birth. The form contained a Privacy Act Statement to tell you why the information was needed, and it implied that every step would be taken to protect your personal information from unauthorized disclosure.

But as you know, the world we live in is changing fast! Information flow is easier and faster. Paper records have morphed into electronic records, and what used to take time to disseminate can now be done in an instant with the push of a button. Thumb drives have replaced floppy disks and personal information is stored in many forms.

Recent e-government mandates require transparency of privacy programs. The federal government is committed to the goal of having its citizens understand what private information is collected and how that information is used. At the same time, the government wants federal employees to ensure that safeguards are deployed to protect personal information.

The DON has been fortunate to team with the Naval Audit Service, which also seeks to ensure that the Department adopts and adheres to best privacy practices. During recent audits, auditors found that DON recycling bins and waste containers were filled with papers containing personally identifiable information, seemingly without a thought about better protecting this data. Some people mistakenly think that the recycler is responsible for shredding or burning these documents. But the reality is — they are not. We, the users, are responsible, and we must be vigilant in the handling of personal information!

Policy Guidance

The Office of Management and Budget, the policy official for the Privacy Act, has been working on a new notification requirement since the report of the Department of Veterans Affairs security breach involving 27 million veterans in 2006. OMB is working with agencies to bring a halt to breaches by establishing new business practices to protect privacy.

OMB is considering holding employees accountable when their actions result in the loss of PII. In the future, the lack of attention to the secure use, storage and disposal of private information may result in punitive action. Just imagine having a stellar career change in an instant — as a result of a security breach that costs you your job or a promotion!

It is apparent that we have come to rely on the Social Security Number as the primary identifier. But the Social Security Administration states that this was not its intended use. While it is evident that a change is needed, it will take time and money to retool federal IT systems to remove the SSN as a personal identifier.

While agencies are currently providing comments on recommendations regarding use of a different identifier, the bottom line is that the cost of breaches on all levels — monetary, embarrassment, and risk to privacy and identity theft — is too high. Agencies will be required to take aggressive steps to eliminate the potential for breaches of PII.

The solution to eliminating breaches begins with you! Why? Because you use, disseminate, collect, and manage great amounts of personal information, and it is your diligence that will enable the DON to minimize loss of PII.

Alerting DON personnel to their role and responsibility in protecting privacy is key to minimizing and possibly eliminating breaches. To this end, the DON has had privacy standdown

training and developed training materials, ads, plan of the day notes, and other tools to get the word out. Most can be downloaded from the DON Privacy Office Web site at http://privacy.navy.mil.

In the DON, more than 220 Navy and Marine Corps systems contain personally identifiable information, which is retrieved by an individual's name and personal identifier. For these systems, the DON is performing Privacy Impact Assessments, a tool originally developed by the Internal Revenue Service to ensure the integrity and safety of the myriad of documents containing personal information that it receives to compute taxes.

The Department asks you to ensure that breaches are eliminated and privacy is protected by following sound business practices to protect PII, including:

- Be sure to secure! Make sure documents containing PII are not accessible to compromise or loss.
- Encrypt, Encrypt, Encrypt! When transmitting data, make sure that you use a secure connection. If you don't know how to do it, find out soon. The procedure is easily learned.
- If you don't need the information, don't take it with you — electronically or on paper!
- Once you have read it, shred it! Don't let it stack up on you.
- Browse the World Wide Web smartly! Make sure that your security and privacy settings are at an appropriate level.
- Make your passwords complex! The passwords used for e-mail, online banking, and other transactions that contain private information should not be simple or easily guessed. The best passwords are a blend of special characters, numbers, and lower and uppercase letters.

Our motto regarding private information must be: ***If we collect it, we must protect it!***

Doris Lama is the Department of the Navy's Freedom of Information Act and Privacy Act policy officer. Richard Wolfe is responsible for privacy in the information assurance/identity management/privacy section of the DON Chief Information Officer. CHIPS

TEN RULES To Protect Personal Information

- DO NOT be afraid to challenge "anyone" who asks to see Privacy Act information that you are responsible for.
- DO NOT maintain records longer than permitted under records disposal.
- DO NOT destroy records before disposal requirements are met.
- DO NOT place unauthorized documents in Privacy Act record systems.
- DO NOT co-mingle information about different individuals in the same file.
- DO NOT transmit personal data without ensuring it is properly marked. Use "FOR OFFICIAL USE ONLY – PRIVACY SENSITIVE."
- DO NOT use interoffice envelopes to mail privacy data.
- DO NOT place privacy data on shared drives, multi-access calendars, the Intranet or Internet that can be accessed by individuals who do not have an official need to know.
- DO NOT create a new system of records without first consulting your privacy office or Chief of Naval Operations (DNS-36).
- DO NOT hesitate to offer recommendations on how to better effectively manage privacy data.

– DON Privacy Office

First CTN "A" School Launches at CID Corry Station

By Darlene Goodwin

The first class of the new Cryptologic Technician Networks "A" School convened at the Center for Information Dominance (CID) Corry Station, Feb. 26. Ten Sailors in paygrades E-1 through E-3 are enrolled in the course to learn basic network and networking fundamentals, including devices, topology and security issues.

CID Commanding Officer Capt. Kevin R. Hooley said the training prepares Sailors for complex and mission critical computer network operations in the information warfare domain.

"Information warfare is integral to 21st century Naval operations — combat, peacekeeping, stability and humanitarian," Hooley said. "This course prepares Sailors for these duties in the ever-growing cyber battlespace."

The CTN rating was originally manned with Sailors selected to convert from other CT ratings. Following several rounds of CT-only conversions, the rating is now open to Sailors in any rating who qualify and pass the review process. The first CTN "A" School students are also the first new CTN accessions into the Navy. Cryptologic Technician Networks Seaman Recruit (CTNSR) Casey Denton called it an "amazing milestone" to be a part of.

"CTNs in the future will look to us as pioneers (who built) the pathway they will follow," Denton said. "It is a huge responsibility that we have agreed to take on, and we are all ready and willing to stand up to the challenge."

According to Hooley, the new rating and training were developed in response to emergent warfare requirements and to pace ever advancing technology.

"This evolution bears witness to the dynamic and rapidly responsive nature of our manpower, personnel, training and education system and the Navy's revolution in training," he said. "Combatant commanders and national authorities stated the need for warfare expertise in cyberspace, and in very short order, this new rating was established and formal training implemented."

Course instructor CTN1 (AW) Michael Hawley says the Navy can expect a great product from the new "A" school. "Our goal is to provide the fleet with a Sailor that can make an immediate impact," Hawley said. "And, we fully intend to reach our goal."

CTN "A" School student CTNSR Nancy Pugh is ready to help make that happen. Expressing appreciation to the Navy and nation for the opportunity she has been given, she said, "I'm very proud to be where I am now, knowing that my possibilities are endless, (having been) selected and entrusted to serve the U.S. Navy as a CTN."

CTN "A" School students prepare to begin their new course at the CID Corry Station. Photo by Darlene Goodwin. For related news about the CID, visit the command's Navy NewsStand page at "http://www.news.navy.mil/local/corry/."

Darlene Goodwin is the CID public affairs officer. CHIPS